SCIENCE POLICY RESEARCH UNIT

SPRU Working Paper Series

SWPS 2020–10 (June)

Research Note

The Saga of the Covid-19 Contact Tracing Apps: Lessons for Data Governance

Maria Savona

UNIVERSITY OF SUSSEX | BUSINESS SCHOOL

SPRU Working Paper Series (ISSN 2057-6668)

The SPRU Working Paper Series aims to accelerate the public availability of the research undertaken by SPRU-associated people, and other research that is of considerable interest within SPRU, providing access to early copies of SPRU research.

Guidelines for authors

Papers should be submitted to swps@sussex.ac.uk as a PDF or Word file. The first page should include: title, abstract, keywords, and authors' names and affiliations. The paper will be considered for publication by an Associate Editor, who may ask two referees to provide a light review. We aim to send referee reports within three weeks from submission. Authors may be requested to submit a revised version of the paper with a reply to the referees' comments to swps@sussex.ac.uk. The Editors make the final decision on the inclusion of the paper in the series. When submitting, the authors should indicate if the paper has already undergone peer-review (in other series, journals, or books), in which case the Editors may decide to skip the review process. Once the paper is included in the SWPS, the authors maintain the copyright.

Websites

UoS: **www.sussex.ac.uk/spru/research/swps**
SSRN: **www.ssrn.com/link/SPRU-RES.html**
IDEAS: **ideas.repec.org/s/sru/ssewps.html**

The Saga of the Covid-19 Contact Tracing Apps:

What Lessons for Data Governance?

Professor Maria Savona
Science Policy Research Unit, University of Sussex
June 2020[1]

Abstract

This note selectively unpacks the rapid evolution of the (Western) debate around the opportunity to deploy contact tracing apps, alongside other digital tools such as apps for symptoms sharing and immunity certificates to mitigate the Covid-19 pandemics. I do so from the perspective of a social scientist interested in the implications of the development of digital tools at times of emergency in terms of data governance. I argue that a more articulated reflection is needed towards the development of a healthy institutional structure that regulates the role of large tech platforms, such as Google and Apple (G&A), and public institutions, in governing data, particularly when health data and public value are involved. I unravel the saga of contact tracing apps in the UK and EU, looking at the technical, legal and ethical aspects and I attempt to draw more general lessons for data governance.

Keywords: Contact tracing apps, data governance, digital applications, digital exclusion, public trust.
JEL codes: O33; O36; O38; L51

Introduction

In a context of any disease outbreak , provided that people rely on their tested/diagnosed rather than self-reported status, a *digital contact tracing application* is supposed to be more effective than a *manual contact tracing procedure*, as it immediately identifies and informs all the contacted and potentially infected people in real time, and has the potential to reduce the R. Also, a digital app would alert all those contacts that are unknown to the potential spreader, rather than relying on their memory and self-reporting. The automation of the contract tracing procedure and the digitalisation of the information in this case are ideally what technical change is supposed to achieve: providing solutions to address pressing societal challenges.

At exceptional times of public health emergency such as the current Covid-19 pandemic, Taiwan, South Korea and Singapore, among other East Asian countries, have managed to limit the spread of the first wave contagion better than other countries. Besides immediate and strict lockdowns, they have resorted to the digital tracking of individuals with symptoms, identifying and isolating their contacts, and ensured the golden mix of high rate of *testing*, contact *tracing*, and immediate *isolation/treatment*. Most likely due to the experience of earlier outbreaks, these countries have done better than others with sluggish reactions and substantive unpreparedness, such as the US and the UK.

[1] I am grateful to Josh Moon, Simone Vannuccini and the Editors of the SWPS for their constructive remarks and suggestions on an earlier draft of this note. I am also grateful for the very insightful comments from the participants to the SPRU virtual Wednesday seminar (24 June 2020). All omissions and simplifications are my responsibility.

Lanier and Weyl (2020) have promptly acknowledged the Taiwanese strategy and described the *proto-model* of the Taiwanese contact tracing app. This consisted of a platform developed in cooperation among the digital minister, a group of local entrepreneurs and the *g0v movement*, and used voluntarily by citizens to share symptoms and locations, promptly verified by the local health centres and collated centrally. The protocol used relies on a centralised repository of data, facilitated by a shared sense of relevant public purpose, and a substantial degree of trust in the government, which Audrey Tang, the young and industrious digital minister of Taiwan, certainly enjoys. This was on the 20th of March, a pre-history in the development of the debate, considering the unprecedented pace at which the pandemics has forced the mobilisation of governments, both in response to the WHO Country and Technical Guidance and the country-specific spread of contagion.

Indeed, the use of digital technology, that so deeply pervades the tissue of our societies, raises as many challenges as it overcomes, around personal data collection and storage, user consent, and surveillance, particularly in the context of health data. Nothing is more dangerous for a democracy, ideally characterised by a safe-space for public scrutiny and monitoring of the government's accountability, than hiding behind false dilemmas such as "public health versus privacy" at times of emergency. Emergencies have gloomy historical precedents of exceptional public interventions, reduced space for public debates, a lingering sense of threat that impinge on thoroughly scrutinised actions, that favour emotional responses.

Here I selectively unpack the rapid evolution of the (Western) debate around the opportunity of deploy contact tracing apps, alongside other digital tools such as apps for symptoms sharing and immunity certificates.[2] I do so in the attempt of articulating the debate from the perspective of a social scientist interested in more general implications for the governance of data, including aspects of data value. The aim is to factor in the potential exacerbation of the current digital exclusion, particularly in a context of emergency, when anything deployed in haste, by surfing the waves of the public's panic and lacking of an appropriate debate and oversight, is hardly reversible. The pace of the debate, and the role of different actors, including experts, policy makers, adopters, civil servants and independent institutions, who have voiced their concerns at different stages have all contributed to an intriguing saga.

The note is structured to examine the technical, legal and ethical aspects of the saga, to keep track of the main actors involved, and to unveil the plot in a loose chronological order. There is no pretension of exhaustivity of all the relevant issues to be accounted for, rather a selection of them, a review of the main sources feeding the debate, and a plea for multi-disciplinarity as a safety net against biased discourses.

The salient moments of the saga: The technical and regulatory issues at stake

Unveiling the salient moment of the plot

The box below summarises the salient chronological moments of the Coronavirus pandemics with respect to development of the digital mitigation tools as discussed in the note.

[2] While the main focus of this note is on contact tracing apps, the issues raised and discussed by and large apply to public health agencies or universities-developed apps that allow people to share their symptoms, such as the Kings College ZOE app; and to the potential use of digital immunity "passports", that would allow people to get back to work or travel.

Feb-March: Deployment of digital tools to mitigate pandemics in Taiwan, South Korea, Singapore, China;
April 3rd: first version of DP3T protocol, international network of academics led by EPFL;
April - : European institutions restlessly debating and releasing guidelines: the issue of centralized versus decentralized solutions dominates the debate;
Mid-April: Google and Apple launch joint Android and iOS support to a decentralized solution for contact tracing apps;
May: UK Parliamentary Joint Committee on Human Rights, on Human Rights and the Government's Response to Covid-19: Digital Contact Tracing, based on the Coronavirus Safeguards Bill 2020;
May-June: launch of the contact tracing apps in a few EU countries;
June - : some EU countries freeze or reconvert the apps due to data protection issue: Netherlands, Lithuania, Denmark, Germany, UK

There are two main technical aspects that dominated the debate over the time span above. These relate to the use of a decentralised or centralised protocol and, more in general, how to ensure the interoperability of the API that supports the contact tracing apps. The technical characteristics interwove with the regulatory issues and the implications in terms of digital rights.

Decentralised versus centralised protocols and beyond

Since March 2020, the mounting debate around the design, deployment, regulation and – albeit less so – the *effectiveness* of digital contact tracing apps, has been pervaded by the narrative that public health is more important than privacy when time is an issue. Indeed, at the time of writing, there is still a heated debate in the public domain on the trade-offs between the *public health* challenge of containing the spread, the *pace* at which this should happen to allow economies to re-start, in this and subsequent waves to avoid deep recessions, and the imperative of preserving privacy, avoiding mission creep, and the risk of data leakages.

A remarkable international academic team, led by Carmela Troncoso at EPFL and including developers of technical protocols, privacy engineers and law experts, has jointly developed a Decentralised Privacy-Preserving Proximity Tracing (DP3T) protocol to support contact tracing apps. This remains fully decentralised and therefore ideally apt to preserve privacy, and avoid any non-purposeful usage of the data gathered (see White paper by Troncoso et al., 2020, whose first version (3rd of April 2020) was released ahead of the one announced by Apple and Google).

In a nutshell, a decentralised protocol allows individual data to be left in the devices, whilst a centralised solution collects data in a central repository, such as a public health authority. The **technical specification** of the DP3T protocol would ensure all the GDPR principles of data minimisation, purpose limitation, storage limitation, integrity and confidentiality, lawfulness, fairness and transparency and accountability and accuracy. [3] A decentralised solution is technically (though perhaps not politically) preferred to a centralised one in terms of privacy-preserving. However, it should be noted that, even if the app does not record personal data such as name and email address, it is still linked to a phone or an IP address, which are indeed

[3] It is worth recalling that these are fundamental principles of data protection under GDPR (and mirrored in the future UK GDPR after Brexit). These are also those considered in the Guidelines 04/2020 of the EDPB mentioned below.

personal data. Experts have therefore not ruled out the possibility to link the data collected by the app to some personal information, hence re-identification (data are pseudo-anonymous rather than fully anonymous, making public trust crucial for its adoption). Conversely, a centralised solution might facilitate data collection and analysis, for instance for (compatible secondary) research purpose. A centralised solution that supports contact tracing apps has since been adopted in France, and originally considered in Italy, Germany, Denmark (which then opted for a decentralised approach) and the UK (where the debate is ongoing).

In parallel, the European governments have been debating internally and within the European institutions, leading to a fragmentation of country-specific approaches, partly due to the complexity of the issue and a mere lack of thorough and reliable information. A useful summary of the rapid paced debate within the European Parliament, Council, and the Commission is provided by Gabriela Zanfir-Fortuna in "Privacy and Pandemics. The European Union's Data-Based Policy Against the Pandemics" (April 30, 2020), which also examines the Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covind-19 outbreak, adopted on the 21st of April by the European Data Protection Board (EDPB).

With the main exceptions of France, UK so far and Denmark, a higher number of European countries are now developing, or have already launched, apps relying on the DP3T protocol. [4] Interestingly, Apple and Google supported this protocol within days from its first release, and announced steps to make the app available on Androids and iOS. This has been globally welcome as an important step to ensure the scaling up of the app's adoption. However, it is also a crucial node of the saga, which will be reprised below.

The heated debate between supporters of decentralised and centralised solutions, mainly limited to the technical characteristics of the app, more or less privacy preserving, is only part of the story. More broadly, what is at stake is what ultimately leads people to adopt and install on their devices a formal surveillance tool and whether this is proportionate to its (so far untested) effectiveness. This arguably depends on the extent to which people trust their governments, public health institutions, or, indeed, the large tech companies that might have different interests at stake.

Interoperability

For the sake of technically illiterate social scientists, interoperability allows that digital systems, including protocols, data, content, platforms and downstream services, have elements of standardisation that make them working together. Interoperability is widely considered as contributing to a transparent, trustworthy environment for citizens who face the choice of opting in a contact (or symptom, or immunity) tracing app, across devices, and countries.

Application Programming Interfaces (APIs) are a crucial intermediate element in the data value chain, and one of the main mechanisms to create barriers to entry to competitors and third party using data.[5] Changing APIs in a direction of standardisation or further restriction might mean

[4] The European Commission has in the meantime launched a Joint European Roadmap towards lifting COVID-19 containment measures that partly relies on contact tracing apps (See accompanying measures, ns. 1 & 2) though seems to prefer the decentralised protocol to the centralised one, after a swift U-turn with respect to the very initial approach.

[5] It is so, as they allow "efficient repurposing of the non-rivalrous goods of data and networks" (Riley, 2020, p. 99) by allowing access to data and function to downstream markets.

either a pro-competitive move or a locking in strategy to hamper access to third parties. Enforcing interoperability in APIs can avoid antitrust laws to be hand-tightened in having to assess a "legitimate pro-security API change and an anti-competitive act disguised as a pro-privacy move" (Riley, 2020, p. 104).

The E-Health Network has published (13th of May 2020) the Interoperability guidelines for approved contact tracing mobile applications in the EU. The aim is to further develop the interoperability framework in the EU in view of the approval of mobile contact tracing apps. For the purpose of easing cross-border trade and travel, all member states should ensure interoperability to facilitate all app users to rely on a single app, regardless of where they are based and what each member state decides to adopt, whether a fully decentralised app or a centralised one. The EU interoperability protocols should therefore be adapted to allow an interoperable contact-tracing apps, that is standardised with respect to epidemiological criteria. Such interoperability not only allows national lockdown lifting but also borders re-opening, as it facilitates interoperability across national apps, cross-borders contact tracing, as well as data exchange among national health authorities, which depends on how many countries subscribe the centralised app.

There is convergence in considering that enforcing interoperability across several relevant dimensions within the digital platform system, and particularly on large tech might help achieving a trustworthy environment, particularly at times of emergency, when trust is key. I wonder whether this is an unprecedented opportunity at a critical moment, for competition and trust laws to be enforced once the app is fully relying on Google and Apple's operation systems.

The recipients of public trust and adoption rates

One of the most controversial and yet crucial points regulated by the EDPB is the use of health data for research purposes. Data for research purposes can be of *primary use* (data directly collected for the purpose of scientific studies) or of *secondary use* (data that consists of further processing of data initially collected for another purpose).

Recall that a centralised solution allows data storage (and processing) on a central backend server, ideally allowing for '*compatible purposes for secondary use*' (EDPB Guidelines 3/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak) within the boundaries of privacy-preserving.

Arguably, data collected by public health institutions in the context of Covid-19 symptoms and contact tracing are of this second type, if subsequently allowed to be re-used for research purposes as it seems. At the same time, one would expect that a transparent communication on the (limited) purposes of citizens' health data use is likely to be an important leverage to build up trust and increase likelihood of adoption. This is what the EDPB considers "compatible purposes for secondary use", that are those of public research to mitigate Covid-19, compatible with the purpose of tracing symptoms and the contacts of the symptomatic and positive individual.[6] High transparency is needed in this context, which implies a clear regulation of the secondary use for research purposes.

[6] However, the EDPB has so far not given a specific guidance on what are the compatibility of purposes in this context (Zanfir-Fortuna, 2020).

However, a preliminary study by Simko et al. (2020) finds that a high percentage of the (unrepresentative) sample of the population surveyed did not trust their government would delete their data at the end of the emergency (72%) or would use their data only for contact tracing purposes (65%) though a good third of the respondents (26%) would expect their data to be used for research purposes related to pandemic mitigation.

Despite these preliminary results, it is somewhat surprising that people are more at ease with having their Apple and Google platforms, rather than their government (or their public health agencies, and even less the WHO or the UN), involved in contact-tracing apps and collecting their data for public purpose. If further corroborated, this is a very interesting and policy informing finding. I will return on this below.

To summarise, over the last three months, and at a remarkably fast pace, there has been a substantial fragmentation of national digital response to the pandemics, an understandable shock that permeated the public debate, and a restless work at the European level to guide and regulate the public response to the emergency. I have highlighted three main issues on the digital response to Covid-19 and that stood-out in the debate. The first one is the governments' choice and the European guidelines on the use of a decentralised or centralised approach to the contact tracing app, with different implications for personal data protection and other GDPR principles. The second one is the prospective enforcement of interoperability to ensure all these digital tools to be operated across-country. The third one is the extent to which there has been transparency of communication on how the personal data collected are to be re-used for compatible secondary purposes, in line with the EU guidelines. All of these issues affect the level of trust that citizens have in public institutions, hence the level of adoption of the app, which is a key ingredient for its effectiveness.

Striking the right balance between techno-determinist and techno-phobic to build up public trust: the UK saga

In the UK, the debate has been intense, among different circles, including academics, particularly privacy law and engineering experts, and independent institutions such as the Ada Lovelace Institute. A remarkably balanced view is offered in the Rapid Evidence Review 'Exit through the App Store', which unpacks and systematises the multiple layers of risks of rushing into a national deployment of contact tracing apps, highlighted also by Robin Mansell in her blog Coronavirus contact tracing apps: A proportionate response?

The deployment of **symptoms' tracking, contact tracing and immunity passports** covered in the Ada Lovelace Institute's report should all be assessed against technical, ethical and legal issues. These go well beyond the issue of privacy, which seems to have become the trojan horse and perhaps a misleading target of this debate. The public response to the health emergency, despite the fast pace required, should be **effective**, **accurate**, **proportionate** and consistent with the public expectations of trust and trustworthiness. Getting the intervention wrong the first time will lead to an irreversible damage to public trust and undermine any further intervention. Building trust gradually, by being transparent about the risks and the uncertainties, is a much preferred solution[7].

[7] As emerged in the debate on COVID-19, Artificial Intelligence and Data Governance: A Conversation with Lord Tim Clement-Jones hosted by the British Institute of International and Comparative Law.

First, as mentioned, the **technical specification** of the apps should ensure all the GDPR principles of data minimisation, purpose limitation, storage limitation, integrity and confidentiality, lawfulness, fairness and transparency and accountability and accuracy. The use of these apps should be proportionate to their objective, and limited to the time of emergency. Even so, the effectiveness of these apps is not guaranteed, as they much rely on the rate of **adoption**, which in turn depends on **trust**, and on the availability of tests to avoid false positive and a strategic use of symptoms.

Second, the ethical and social issues are much more uncertain: the adoption of these apps should not be made **mandatory**, and no one should be **penalised for not adopting**, including those who cannot adopt, due to **digital exclusion**. The shares of the population which are not in the position to adopt digital tools, are also likely to be those most vulnerable and at risk, due to general health inequality. This applies also to the controversial introduction of the immunity passport, so far not yet implemented. At any rate, prospectively, the introduction of immunity passports should not be used as condition to be recruited, to travel or be admitted to public places, as this risks to disrupt public trust and increase surveillance, at least in western democracies.

Third, the legal issues involved here should be considered **within the context of human rights** rather than limited to privacy rights. The Bill of Safeguard, by Lillian Edward and co-authors, mentioned also in the Joint Committee on Human Rights, which has informed the Human Rights and the Government's Response to Covid-19: Digital Contact Tracing, has put forward clear principles of proportionality and legal safeguard. In particular, it is recommended that a national contact tracing app should not be rolled out in the absence of guaranteed (1) Efficacy and Proportionality (unless benefits are clear, the scale and level of data collection is not justifiable, including risks to privacy); (2) Primary legislation (on privacy and human rights more in general to avoid violation of purpose limitation or mission creep for instance); (3) Oversight (presence of an independent body to oversee the use of these apps); (4) Child safeguard; (5) Efficacy review; (6) Transparency.

The recommendation of the Joint Committee on Human Rights, within the Third Report of Session 2019-21 on "Human Rights and the Government's Response to Covid-19: Digital Contact Tracing" have been considered (though not adopted) by the Government.[8] The recommendation of the Ada Lovelace Institute to establish an independent Technical Advisory Group of Expert (TAGE) alongside the SAGE, the Scientific Advisory Group of Expert and the recommendations of the Joint Committee on Human Rights have been considered too. At time of writing, contact tracing apps have been piloted in the Isle of Wight, with controversial outcomes, and the NHSX has postponed to the autumn the launch of a contact tracing app, based on the Google/Apple API. The UK Government is requiring the use of G&A API to be conditional to specific characteristics, unknown at present.

What lessons for data governance?

[8] According to a recent column in The Conversation (Why we need to know more about the UK government's COVID-19 data project – and the companies working on it) the Government has stated that "Existing legislation (especially the Data Protection Act 2018 and the Human Rights Act 1998), our commitment towards transparency, and the commitments (…) previously set out ensure high levels of security and privacy, will provide the public with the right protection and give them clarity and confidence to download and use the app to support our national effort to tackle COVID-19. We will continue to work with the Information Commissioners Office and the National Cyber Security Centre and use our Ethics Advisory Board to review our processes, provide rightful challenge and informed advice as the Test and Trace programme is rolled out nationally in the coming weeks".

A summary of the technical, regulatory and ethical issues in the saga

The fast unravelling of the contact tracing saga since mid-March 2020 has provided some ground for a first-hand reflection on the wider issue of data governance, for social scientists interested in the economic and social impact of digital technology. A balanced view is all the more needed at times of emergency, to avoid both an irreversible, detrimental disruption of public trust, and a misleading, simplistic framing of the debate around a trade-off between public health and privacy. In addition, this debate has clearly shown that getting the narrative right needs a multidisciplinary expertise.

I will get back to the aspects highlighted above, namely the technical, legal and ethical issues that have characterised the debate so far. I will then also consider the involvement of the large tech, which is a key ingredient when drawing lessons for data governance.

1. **Technically**, the public should be in a position to understand what are the technical features, effectiveness and the (hopefully limited) purpose of any digital tool they (hopefully voluntarily) decide to adopt. Understanding what 'privacy by design' means and what are the side-effects of a centralised protocol, or a back-end central data repository is crucial. Similarly, it is on data scientists, privacy engineers, and internet law experts to divulge the importance of interoperability, not only in the context of contact tracing apps, but within the system of digital platforms. Technical literacy is a fundamental ingredient to ensure that people make informed choices, and ultimately to ensure a minimal adoption rate.

2. **Legally,** as effectively put forward in the Bill of Safeguard, and partly also within the European institutions, the deployment of digital tools should be safeguarded on the basis of human rights, rather than privacy rights only. This means that an informed public debate at the parliamentary level, primary legislation, and independent oversight bodies, are needed. Clarity and transparency on the regulation of the 'compatible purposes for secondary use' of personal health data are crucial ingredients towards public trust building.

3. From the **ethical and social perspective**, it is important to predict first, and regulate accordingly, the potential side effects of digital exclusion and potential discrimination from the use of digital tools for tracking, tracing and certificating immunity. Low income, vulnerable citizens might not be in the position to access information, increase their awareness and develop agency over their personal health (and location) data. None of the digital solutions considered here should end up discriminating or further polarising inequalities, for instance in labour markets or in society at large.

Google and Apple: The main actors in the saga, after all?

Google and Apple will support the decentralised solution to contact tracing apps developed in the DP3T protocol. Technically, they won't be able to access any personal data, as this data remains in adopters' devices. G&A allow the adoption of health-related apps on a global scale, as smart phones are pretty much all running either on Androids or iOS systems. As such, G&A's involvement has gone pretty much unquestioned, rather welcome as a humble step in support of privacy and public health.

However, I am surprised that the role of large techs in this landscape has not been sufficiently put under scrutiny in the public debate, for instance by institutions such as the Ada Lovelace Institute. Some preliminary surveys across the EU and US have shown concerning evidence, that, if further corroborated, shows a neat tendency of citizens to trust G&A more than governments when it comes to data collection and use. Not only should we reflect on the state of the art of public's awareness of what is – at least in principle – a *public value* against a *private interest*, but predict with a reasonable degree of accuracy what are the consequences of the public confiding their trust in a large tech more than in their own government, when one compares the degrees to which they are respectively accountable to societies. All this despite the recent history of private surveillance and massive power and equity value concentration, well documented in several academic and grey literature, and that I recall briefly in an earlier column.

There are only a few critical voices that support these concerns, including the established Financial Times, in Waters (2020), Big Tech search of a way back into health care (13 May 2020), more radical outlets (among others, Magalhães and Couldry (2020) on the Jacobin, Tech Giants are using this crisis to colonise the welfare system (by 27 April 2020), and others such as Greig (2020) on The Conversation (Contact-tracing apps: Apple dictating policies to nations won't help its EU anti-trust probe, June 2020).

Without getting into any conspiracy theory, I wish to invite reflection on the following:

First, to ensure adoption and installation of health-related apps, G&A did not have much choice but supporting a decentralised solution. This can easily be seen as a welcome, salvific intervention and yet be close to what the literature has called by Pontecraft (2016), among many others, as a "symbolic", rather than a "substantive" corporate social responsibility (CSR), where a *substantive* CSR is supposed to genuinely supporting the common good, while the *symbolic* is a self-serving façade, towards improving (or re-establishing in some case) reputation, but actually aiming to enhance profits.

Second, once installed, and having a quasi-monopoly of operating systems, G&A and all their third-party upstream and downstream satellite companies will be sitting on an immense, additional, pot of highly valuable data. As mentioned, even in the case of a decentralised solution, it is not difficult to navigate towards re-identification. If we factor in that one of their main value extraction gains is data feedback loop[9], it is not surprising that they embrace such a solution to enter a new trove of data. Rather than further speculating, this is just a note of caution and a plea on being aware of potential risks and open the public debate on this too.

Third, the involvement of G&A should be regulated at the international level. In this context, self-endowing with an ethical self-regulatory body, in the vein of what Facebook has been recently doing (Vaidhyanathan, 2020) boils down to ethical washing, and by no means can replace the enforcement of international law.[10]

In sum, transparency and accountability are the main keywords to use here, if trust is a key ingredient in the whole saga, and one that is desperately needed in the post-Covid19 reconstruction. The development of digital tools to tackle emergencies should be a clear and transparent process, there needs to be primary legislation following public scrutiny of

[9] Thanks to Simone Vannuccini for this reflection.

[10] As emerged in the debate on COVID-19, Artificial Intelligence and Data Governance: A Conversation with Lord Tim Clement-Jones hosted by the British Institute of International and Comparative Law.

proposals. This will help build understanding and trust among the public which will be absolutely key if the track and trace programme is to be taken up by a sufficient portion of the public.

Taiwan might be a first mover in the direction of creating a complex institutional architecture to regulate and manage an effective government response, though trust in public institutions seems to be a necessary (albeit most likely not sufficient) condition for this to be successful. A Euro-centric, certainly fundamental, institutional safeguard of privacy seems not to fully paralleled by the actual level of trust that citizens have in their governments. We should be asking why this is the case. This crisis seems to be an unprecedented occasion to learn more.

References

Ada Lovelace Institute (2020). Covid-19 Rapid Evidence Review: Exit Through the App Store? https://www.adalovelaceinstitute.org/our-work/covid-19/covid-19-exit-through-the-app-store/.

Apple and Google partner on the use of contact tracing technology (April 10, 2020).

Boiten Eerke, Why we need to know more about the UK government's Covid-19 data project - and the companies working on it. The Conversation, June 24 2020

Edwards, Lillian, Michael Veale, Orla Lynskey, Rachel Coldicutt, Nóra Ni Loideain, Frederike Kaltheuner, Marion Oswald, Rossana Ducato, Burkhard Schafer, Aileen McHarg, Elizabeth Renieris, Elettra Bietti (2020). The Coronavirus (Safeguards) Bill 2020:
Proposed protections for digital interventions and in relation to immunity certificates, 10.31228/osf.io/yc6xu.

E-Health Network (2020) Interoperability guidelines for approved contact tracing mobile applications in the EU.

European Data Protection Board (2020). Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21 April 2020.

Greig, Paul (2020). Contact-tracing apps: Apple dictating policies to nations won't help its EU anti-trust probe. The Conversation, June 24 2020.

House of Commons, House of Lords Joint Committee on Human Rights (2020). Human Rights and the Government's response to Covid-19: Digital Contact Tracing. Third Report of Session 2019-21. 6th of May 2020.

Lanier, Jaron and Glen Weyl (2020). How Civic Technology Can Help Stop A Pandemic. Taiwan's Initial Success Is a Model for The Rest of the World. Foreign Affairs, March 20, 2020.

Magalhães, João Carlos and Nick Couldry (2020). Tech Giants are using this crisis to colonize the Welfare System. Jacobin, 27 April 2020.

Mansell, Robin (2020). Coronavirus contact tracing apps - a proportionate response? LSE Blogs, 23 April 2020.

Pontefract, Dan (2016). Faking Corporate Social Responsibility does not fool employees. Forbes, Sept, 24 2016.

Riley, Chris (2020) Unpacking interoperability in competition, Journal of Cyber Policy, 5:1, 94-106, DOI: 10.1080/23738871.2020.1740754

Simko, L, Cako R., Roesner F. and Kohno T. (2020). COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences. May 2020, https://seclab.cs.washington.edu/research/covid19/

Troncoso, Carmela, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Čapkun, David Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel Smart, Aysajan Abidin, Seda Gürses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Prof. Ciro Cattuto, Dr. Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, José Pereira, (2020). White Paper on Decentralised Privacy-Preserving Proximity Tracing. https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

Zanfir-Fortuna, Gabriela (2020). European Union Data-Based Policy Against the Pandemics, Explained. Future of Privacy Forum, April 30 2020.

Vaidhyanathan, Siva (2020). Facebook and the Folly of Self-Regulation. Wired, 9 May 2020.

Waters, Richard (2020). Big Tech searches for a way back into healthcare. Financial Times Special Report on Future of AI and Digital Healthcare, 17 May 2020.

Recent papers in the SPRUWorking Paper Series:

June

2020-09. Subsidising Innovation over the Business Cycle. *Isabel Busom and Jorge Vélez-Ospina*

2020-08. Going Revolutionary: The Impact of 4IR Technology Development on Firm Performance. *Mario Benassi, Elena Grinza, Francesco Rentocchini and Laura Rondi*

May

2020-07. Accountability and Sustainability Transitions. *Siddharth Sareen and Steven Wolf*

2020-06. Targeting Industrial Policy on Business Services: Rationales and Design for the Case of Chile. *Andrés Madariaga*

2020-05. Pulling Effects in Migrant Entrepreneurship: Does Gender Matter? *Alessandra Colombelli, Elena Grinza, Valentina Meliciani and Mariacristina Rossi*

March

2020-04. The Role of War in Deep Transitions: Exploring Mechanisms, Imprints and Rules in Sociotechnical Systems. *Phil Johnstone and Caitriona McLeish*

2020-03. Niche Acceleration driven by Expectation Dynamics among Niche and Regime Actors: China's Wind and Solar Power Development. *Kejia Yang, Ralitsa Hiteva and Johan Schot*

February

2020-02. Investigating the Role of BNDES as a Tool to Transmit Countercyclical Policy Decisions: Evidence from 2002-2016. *Marco Carreras*

Suggested citation:
Maria Savona (2020). The Saga of the Covid-19 Contact Tracing Apps: Lessons for Data Governance. SPRU Working Paper Series (SWPS), 2020-10: 1-12. ISSN 2057-6668. Available at: www.sussex.ac.uk/spru/swps2020-10

Science Policy Research Unit
University of Sussex, Falmer
Brighton BN1 9SL
United Kingdom

SPRU website: **www.sussex.ac.uk/business-school/spru**
SWPS website: **www.sussex.ac.uk/business-school/spru/research/swps**
Twitter: **@spru**

UNIVERSITY OF SUSSEX | BUSINESS SCHOOL